

## ABSTRACT

A method and systems for information security threat identification, management, and analysis, including identifying and managing threats posed by senders of unsolicited e-mail, pirates, hackers, and virus-spreaders. Methods are provided for identifying and facilitating legal action against a sender of unsolicited e-mail. A secure evidence repository can be used for storing copies of and information regarding unsolicited e-mails in a forensically sound manner. A relational knowledge database can be used for storing copies of and information regarding unsolicited e-mails such that the information can be queried, manipulated, or analyzed.